
SOUTHSIDE VIRGINIA COMMUNITY COLLEGE INFORMATION TECHNOLOGY SECURITY PLAN

IT Systems Security – *IT System Development Life Cycle*

In accordance with the [COV ITRM 501-01](#), IT Systems Development Life Cycle Security document the security related activities that must be adhered to in each phase of the development life cycle for System Office and College IT systems.

Best practices for system development life cycle security are listed below to assist in guiding the System Office and Colleges from project definition through disposal of IT application systems. This document provides an overview of the requirements during each phase. Additional detailed information for IT Project Management may be accessed at these web sites:

VCCS Procedures for Technology Projects and Technology Procurements:
<http://www.vccs.edu/its/procedures/index.htm> (Attachment D 4.1)

The Commonwealth of Virginia Guideline for Project Management:
<http://www.vita.virginia.gov/projects/cpm/templates.cfm> (Attachment D 4.1)

Project Initiation Requirement:

A risk analysis should be conducted based on the initial requirements and mission goals to give an overall view of the security requirements for the IT system. The [IT System and Data Sensitivity Classification](#) process should be completed for the proposed system. There must also be an assessment of the need for collection and maintenance of sensitive data before incorporating such collection and maintenance in IT system requirements. SVCC will reference the current Business Impact Analysis and Risk Analysis surveys, forms, and questionnaires (Section B of the SVCC IT Security Plan, Risk Management) in order to meet this requirement.

Project Definition Requirement:

Security requirements should be developed at the same time system planners define the requirements of the system. The security requirements should be incorporated into design specifications along with verification that the security features developed work properly and are effective. The security applied both logically and physically to the system will be applied as to meet the requirements of the IT Systems Security: *Systems Hardening*, Logical Access Control: *Account Management*, Personnel Security: *Access Determination and Control*, and IT Asset Management: *Configuration Management and Change Control* standards. (Sections: D1, E1, H1, and J3 of the SVCC IT Security Plan respectively)

SOUTHSIDE VIRGINIA COMMUNITY COLLEGE INFORMATION TECHNOLOGY SECURITY PLAN

IT Systems Security – *IT System Development Life Cycle*

Project Implementation Requirement:

The IT system security features should be enabled, configured, tested, and validated. Perform a [Risk Assessment for Technology Systems](#) to assess the risk level of the IT application system. SVCC will meet this requirement as per the Contingency Planning and Business Recovery Program: *Risk Assessment for Information Technology Systems* standard. (Section B5 of the SVCC IT Security Plan)

Project Operation/Maintenance Requirement:

The Operation and Maintenance Phase involves completing the numerous security activities involved with an IT system on a day-to-day basis. SVCC should update the IT System Security Plan to document the IT security controls included in the IT system as implemented to provide adequate protection against IT security risks, and comply with the other requirements of this document.

Backups, training, security awareness, and password management are some examples. SVCC uses the Data Protection: *Data Storage media Protection*, Personnel Security: *Security Awareness and Training*, and Logical Access: *Password Management* standards to address these issues. (Sections: F2, H2 and E2 of the SVCC IT Security Plan, respectively)

Project Operation/Maintenance Requirement:

SVCC will retain data handled by an IT system in accordance with the proper retention procedures. The System Office and Colleges should adhere to the procedures currently in place to address the purging of all data, using software utilities or electromagnetic means, from magnetic storage media such as hard drives, removable disk drives, diskettes, CD-ROMs, zip drives, and other magnetic storage media before they are discarded, in accordance with the [ITRM Standard SEC2003-02.1](#). As per the IT Asset Management: *IT Asset control*, “procedure for removal of data from surplus computer hard drives and electronic media” document. (Section J 1 and Attachment J 1.1 of the SVCC IT Security Plan)